AMENDMENTS TO THE CLAIMS

Please enter the following amendments:

1. (Currently Amended) A storage device comprising:

~~a storage medium for retaining data; and~~

an ordinary data storage unit which stores encrypted contents data;

a secret data storage unit which stores license data containing a contents key for decrypting the encrypted contents data;

a cryptographic processing unit which receives, from a host device, and executes a command corresponding to each of a plurality of sequenced subprocesses produced by dividing each of a series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data between the storage device ~~medium~~ and the host device[[, wherein]];

a controller which inputs and outputs the license data via the cryptographic processing unit and inputs and outputs the encrypted contents data bypassing the cryptographic processing unit; and

a bus for receiving the command from the host device, the bus being deallocated for another command when the command is issued, wherein

the cryptographic processing unit receives commands corresponding to a plurality of subprocesses respectively belonging to two or more different cryptographic input and output processes via the bus ~~and in a time-division manner~~, refers to identifying information attached to the command, identifies to which cryptographic input and output process the command belongs, manages the sequence of commands executed in each cryptographic input and output process, and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command.

2. (Canceled)

3. (Previously Presented) The storage device according to claim 1, wherein

when the cryptographic processing unit receives the incorrectly sequenced command, the cryptographic processing unit interrupts the cryptographic input and output process to which the command belongs.

4. (Previously Presented) The storage device according to claim 1, wherein the number of the cryptographic input and output processes which can be performed simultaneously by the storage device is predetermined in accordance with a performance of the storage device.

5. (Previously Presented) The storage device according to claim 1, wherein in response to a request from the host device, the storage device provides to the host device the maximum number of cryptographic input and output processes which can be performed simultaneously by the storage device.

6. (Original) The storage device according to claim 1, wherein the storage medium comprises a normal data storing unit and a confidential data storing unit, the normal data storing unit storing normal data to be exchanged bypassing the cryptographic processing unit, the

confidential data storing unit storing the secret data to be exchanged via the cryptographic processing unit.

7. (Currently Amended) A storage device comprising:

~~a storage medium for retaining data; and~~

an ordinary data storage unit which stores encrypted contents data;

a secret data storage unit which stores license data containing a contents key for decrypting the encrypted contents data;

a cryptographic processing unit for receiving, from a host device, and executing a command corresponding to each of the plurality of sequenced subprocesses produced by dividing each of a series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data between the storage device ~~medium~~ and the host device[[,]];

a controller which inputs and outputs the license data via the cryptographic processing unit and inputs and outputs the encrypted contents data bypassing the cryptographic processing unit; and

a bus for receiving the command from the host device, the bus being deallocated for another command when the command is issued,

wherein the cryptographic processing unit receives commands corresponding to a plurality of subprocesses respectively belonging to two or more different cryptographic input and output processes via the bus ~~and in a time-division manner~~, refers to identifying information attached to the command, identifies to which cryptographic input and output process the received command belongs to, and rejects the execution of the command when having detected that the command is an incorrectly sequenced command in the cryptographic input and output process to which the command belongs.

8. (Previously Presented) The storage device according to claim 7, wherein in response to a request from the host device, the storage device provides to the host device the maximum number of cryptographic input and output processes which can be performed simultaneously by the storage device.

9. (Canceled)

10. (Currently Amended) A host device which exchanges encrypted contents data and license data containing a contents key for decrypting the encrypted contents data, with a storage device that is capable of simultaneously performing a plurality of series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data, the host device comprising:

a controller which divides the cryptographic input and output process into a plurality of sequenced subprocesses and issues commands sequentially to the storage device thereby allowing the storage device to execute a subprocess to be executed on the storage-device side; and

a cryptographic processing unit which carries out encryption or decryption that is required of the cryptographic input and output process, wherein the controller inputs and outputs the license data via the cryptographic processing unit and inputs and outputs the encrypted contents data bypassing the cryptographic processing unit, and

when the controller issues a command, the controller attaches identifying information to the command to identify to which one of the plurality of cryptographic input and output processes the command belongs and to manage the sequence of commands executed in each cryptographic input and output process, and

the controller that issues the command via the bus electrically connecting the host device and the storage device deallocates the bus for another command.

11. (Previously Presented) The host device according to claim 10, wherein the controller issues a command to allocate a process system for performing the cryptographic input and output process prior to initiation of the cryptographic input and output process.

12. (Currently Amended) A data input and output method for exchanging encrypted contents data and license data containing a contents key for decrypting the encrypted contents data between a storage device and a host device, wherein, when performing a cryptographic input and output process between [[a]] the host device and [[a]] the storage device, which ~~that~~ is capable of simultaneously performing a plurality of series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data, ~~and storing data to be exchanged through the cryptographic input and output process,~~ the license data is input and output through the cryptographic input and output process, and the encrypted data is input and output bypassing the cryptographic input and output process, the method comprising:

dividing the cryptographic input and output process into a plurality of procedures and allowing the host device to execute a procedure to be executed on the host-device side out of the procedures;

allowing the host device to issue a command to the storage device via a bus for electrically connecting the host device and the storage device in order to make the storage device execute a procedure to be executed on the storage-device side;

allowing the host device to deallocate the bus for another command;

allowing the storage device to receive the command; and

allowing the storage device to execute the command, wherein

identifying information is attached to the command to identify to which one of the plurality of cryptographic input and output processes, being performed simultaneously by the storage device, the command belongs, and

the allowing the storage device to receive the command includes:

determining whether the received command is a correctly sequenced command in the cryptographic input and output process;

accepting the command successfully when the received command has been determined to be a correctly sequenced command; and

rejecting the execution of the received command when the received command has been determined to be an incorrectly sequenced command.

13. (Previously Presented) The data input and output method according to claim 12, further comprising predetermining an upper-limit number of the cryptographic input and output

processes that can be performed simultaneously by the storage device in accordance with performance of the storage device.

14. (Previously Presented) The data input/output method according to claim 12, further comprising:

allowing the storage device to predetermine an upper-limit number of the cryptographic input and output processes that the storage device can perform simultaneously in accordance with its own performance, and

informing the host device of the upper limit.

15. (Previously Presented) The data input and output method according to claim 13, further comprising, prior to performing the cryptographic input and output processes, selecting and allocating identifying information for identifying the cryptographic input and output process to be performed from among the prepared number of pieces of identifying information determined in the determining step.

16. (Previously Presented) The data input and output method according to claim 14, further comprising, prior to performing the cryptographic input and output processes, selecting and allocating identifying information for identifying the cryptographic input and output process to be performed from among the prepared number of pieces of identifying information determined in the determining step.

17. (Canceled)

18. (Previously Presented) The data input and output method according to claim 12, wherein

when the received command has been determined to be an incorrectly sequenced command, the execution of the cryptographic input and output process to which the command belongs is interrupted.